PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059353
(43)Date of publication of application : 25.02.2000

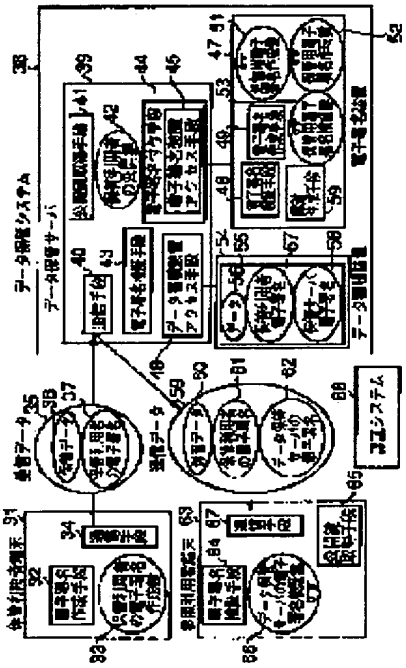
(51)Int.CI. H04L 9/08
G09C 1/00

(21)Application number : 10-225959
(22)Date of filing : 10.08.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : NAKAHARA SHINICHI

(54) DATA STORAGE SYSTEM, DATA STORAGE METHOD AND ITS PROGRAM RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the reliability as a result of verification from being deteriorated due to expiration of validity or invalidation of a public key without the need for many public keys for parties referring to data.
SOLUTION: A user 31 using stored data transmits storage data 36 and its signature 37 to a storage system 38. The system 38 generates a storage signature 58 with respect to the data 36 and the signature 37 by using a storage key after authentication of the signature and stores the storage signature 58 to a storage device 54, reads the signature 58 from the storage device 54 on a reference request from a reference user 63, verifies the signature 58 by the storage key, generates a signature 62 by using a communication key with respect to the data and the signature when the verification is successful, and transmits the data with the signature 62 added thereto to the user 63. The user 63 uses the public key to verify the signature 62 and recognizes its correctness of the received data 60 and the signature 61 simultaneously when the signature is correct.



LEGAL STATUS

[Date of request for examination]	20.10.2000
[Date of sending the examiner's decision of rejection]	07.01.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2003-01922
[Date of requesting appeal against examiner's decision of rejection]	06.02.2003
[Date of extinction of right]	

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－５９３５３

(P２０００－５９３５３A)

(43)公開日　平成12年2月25日(2000.2.25)

(51)Int.Cl.⁷		識別記号	F I			テーマコード(参考)
H04L	9/08		H04L	9/00	601 Z	5K013
G09C	1/00	630	G09C	1/00	630 Z	
					630 F	
			H04L	9/00	601 F	

審査請求　未請求　請求項の数８　ＯＬ　（全８頁）

(21)出願番号　特願平10-225959

(22)出願日　平成10年8月10日(1998.8.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72)発明者　中原　慎一
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(74)代理人　100066153
弁理士　草野　卓　(外1名)

Ｆターム(参考)　5K013 GA05 GA08

(54)【発明の名称】データ保管システム、データ保管方法及びそのプログラム記録媒体

(57)【要約】

【課題】　データ参照者に多数の公開鍵を必要とさせず、公開鍵の有効期限切れや無効化による検証結果の信頼性の低下を防ぐ。

【解決手段】　保管利用者３１は保管データ３６とその署名３７を保管システム３８へ送り、システム３８では、署名検証後、保管用鍵でデータ３６、署名３７に対し保管署名５８を作成して蓄積装置５４に蓄積し、参照利用者６３からの参照要求で、蓄積装置５４から読出し、その署名５８を保管用鍵で検証し、合格すれば、そのデータ、署名に対し、通信用鍵で署名６２を作り、これを付けて利用者６３へ送る。利用者６３は公開鍵で署名６２を検証し、正しければ同時受信データ６０、署名６１の正当性を認める。

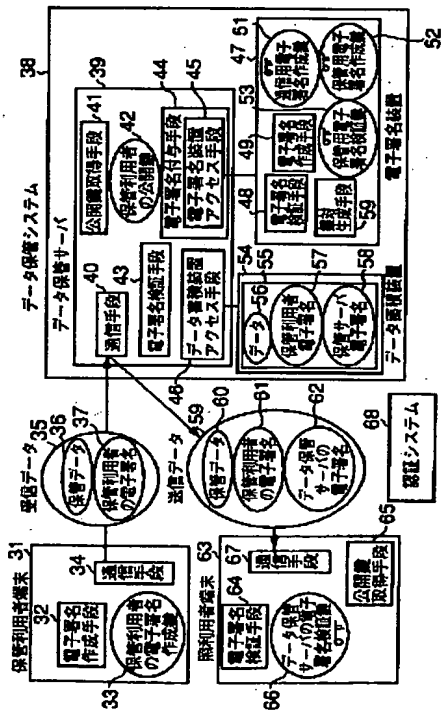


図１

本発明のデータ保管システムの装置構成の実施例

BEST AVAILABLE COPY

1

【特許請求の範囲】

【請求項１】　データ保管サーバと、電子署名装置と、データ蓄積装置とよりなり、

上記データ保管サーバは外部との通信手段と、

上記データ蓄積装置に対するアクセス手段と、上記電子署名装置に対するアクセス手段とを備え、

上記電子署名装置は保管用電子署名作成鍵と保管用電子署名検証鍵を外部からアクセスできないように格納する鍵格納手段と、上記電子署名装置アクセス手段によりアクセスされ、入力されたデータに対し、上記鍵格納手段の電子署名作成鍵で電子署名を作成して戻す電子署名作成手段と、上記電子署名装置アクセス手段によりアクセスされ、入力されたデータに対し上記鍵格納手段の電子署名検証鍵で電子署名の検証を行う電子署名検証手段とを備え、

上記データ蓄積装置は上記データ蓄積装置アクセス手段によりアクセスされ、保管データ及びその電子署名が書込まれ又は読出されるものであることを特徴とするデータ保管システム。

【請求項２】　上記電子署名装置は、その鍵格納手段に通信用電子署名作成鍵をも格納していることを特徴とする請求項１記載のデータ保管システム。

【請求項３】　上記電子署名装置は上記保管用電子署名作成鍵及び上記保管用電子署名検証鍵を生成する手段を備えることを特徴とする請求項１又は２記載のデータ保管システム。

【請求項４】　保管用電子署名作成鍵及びその検証鍵を外部からアクセスできないように格納しておき、

保管要求された保管データに対し、上記保管用電子署名作成鍵により保管用電子署名を作成し、

上記保管データと上記保管用電子署名をデータ蓄積装置に蓄積し、

参照要求された保管データとその保管用電子署名を、上記データ蓄積装置から読出し、

上記読出された保管データとその保管用電子署名に対し、上記保管用電子署名検証鍵により検証することを特徴とするデータ保管方法。

【請求項５】　通信用電子署名作成鍵を格納しておき、

上記保管用電子署名検証鍵による検証結果が合格の保管データに対し、上記通信用電子署名作成用鍵で通信用電子署名を作成し、

上記保管データと上記通信用電子署名を上記参照要求を行った利用者端末へ送信することを特徴とする請求項４記載のデータ保管方法。

【請求項６】　上記利用者端末は受信した上記保管データ及び上記通信用電子署名に対し、電子署名検証用公開鍵で検証することを特徴とする請求項５記載のデータ保管方法。

【請求項７】　保管要求に応じてデータをデータ蓄積装置に蓄積し、参照要求に応じてデータをデータ蓄積装置

2

から読出して出力し、保管用電子署名作成鍵及び保管用電子署名検証鍵を外部からアクセスできないように格納してあるデータ保管システムにおいて、

上記保管要求があると、その保管データに対し、上記保管用電子署名作成鍵により保管用電子署名を作成する処理と、

上記保管データと上記保管用電子署名を上記データ蓄積装置に蓄積する処理と、

上記参照要求があると、その保管データとその保管用電子署名を上記データ蓄積装置から読出す処理と、

上記読出された保管データとその保管用電子署名に対し、上記保管用電子署名検証鍵で検証する処理とをコンピュータにより実行するプログラムを記録した記録媒体。

【請求項８】　上記データ保管システムには通信用電子署名作成鍵も格納されており、

上記保管用電子署名の検証が合格したか否かを判定する処理と、

その判定に合格すると、上記保管データに対し、上記通信用電子署名作成鍵で通信用電子署名を作成する処理と、

上記保管データ、上記通信用電子署名を上記参照要求をした端末へ送出する処理とを上記コンピュータにより実行するプログラムを含むことを特徴とする請求項７記載の記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は保管利用者が保管システムにデータを保管し、参照利用者がそのデータを参照するデータ保管システム、保管方法及びそのプログラム記録媒体に関するものである。

【０００２】

【従来の技術】一般に蓄積したデータに対する不正（盗聴／改竄（かいざん）など）の脅威を防御する方法として、秘匿のために暗号化して保管したり原本とデジタル署名を対応付けて保管し改竄を検知できるようにして保管する方法が広く知られている。そこで用いられる秘匿暗号としては米国のＤＥＳやＲＳＡ暗号や日本のＦＥＡＬやＭＩＳＴＹ暗号が製品として知られており電子署名を実現する暗号技術としては米国ではＤＳＡやＲＳＡ、日本ではＥＳＩＧＮなどが知られるところとなっている。

【０００３】また、改竄・なりすまし検知の方式では公開暗号方式を用い、電子署名作成鍵として秘密鍵が、電子署名検証鍵として公開鍵が用いられる。そして正しい公開鍵を保管あるいは配布するために認証システム（ＣＡと呼ばれる）という第３者機関が用いられ、その発行する公開鍵証明証を用いる通信方式が広く知られている。一方でＣＡに格納された公開鍵（電子署名検証鍵）は一般に公開されているため第３者から公開鍵（電子署

名検証鍵）をもとに秘密鍵（電子署名作成鍵）が解読される脅威にさらされており有効期限が設定されているのが一般である。また秘密鍵を失ったり公開鍵が解読されたりした場合にＣＡが保持している公開鍵を無効化するという手続きがなされる。公開暗号方式を利用する場合、有効期限が過ぎたり無効化された公開鍵は電子署名の検証という処理はできてもその検証結果は信頼できないものとみなされる。また電子署名を作成するための秘密鍵は秘匿する必要があり、外部から内部の情報が検索できないような秘密鍵格納用のＩＣカードなどの専用装置が用いられている。

【０００４】図７は利用者がデータ保管システムにデータの保管を行うときおよびデータを参照するときの従来の装置構成を示しており、図８は利用者端末と保管サーバでのデータ保管時の処理フローを示しており、図９は利用者端末と保管サーバでのデータ参照時の処理フローを示している。従来技術では、まず利用者がデータを保管するとき、保管利用者端末１６上で少なくとも利用者の電子署名作成鍵１９と保管したいデータ２を元に電子署名作成手段１８を用いて電子署名３を作成し（ＳＴＥＰ１）、それらデータ２と電子署名３を含む受信データ１を作成し通信手段１７によってデータ保管システム４へ送信する（ＳＴＥＰ２）。

【０００５】データ保管システム４がその保管利用者のデータ２を保管するとき、少なくとも保管しようとするデータ２と保管利用者により付与された電子署名３を含む受信データ１を通信手段６によって受信したデータ保管サーバ５は（ＳＴＥＰ３）、受信したデータ２および３と公開鍵取得手段７を用いて、認証システム２５から取得した正しい保管利用者の公開鍵８をもとに電子署名検証手段９によりデータが改竄されていないことを確認する（ＳＴＥＰ４）。改竄されていないことを確認した後、データ蓄積装置アクセス手段１０を用いてデータ蓄積装置１１に保管データ２と電子署名３との関連が判るようにデータ対１２として保管する（ＳＴＥＰ５）。

【０００６】一方保管したデータを参照利用者が参照するときには、データ保管システム４は、通信手段６によりデータ参照要求を受け付け（ＳＴＥＰ６）、データ蓄積装置アクセス手段１０を用いて保管データ対１２をデータ蓄積装置１１から読み出す（ＳＴＥＰ７）。そしてデータ対１２の保管データと電子署名および公開鍵取得手段７を用いて認証システム２５から取得した正しい保管利用者の公開鍵８をもとに電子署名検証手段９により保管期間中にデータが改竄されていないことを確認する（ＳＴＥＰ８）。確認後、参照利用者端末２０に少なくとも保管データ１３と保管していた電子署名１４を含んだ送信データ１５として参照利用者端末２０へ送信する（ＳＴＥＰ９）。そして参照利用者端末２０は保管利用者の電子署名１４を含んだ電子データ１５を保管システム４から受信し（ＳＴＥＰ１０）、電子署名取得手段２４によりその時の保管利用者の正しい電子署名検証鍵２３を取得して（ＳＴＥＰ１１）、電子署名検証手段２２により受信したデータ対１３と１４に改竄がないことを検証する（ＳＴＥＰ１２）。この検証で合格になれば正しいデータが参照できたことになる。

【０００７】

【発明が解決しようとする課題】今、データを保管する利用者Ａとデータを参照する利用者Ｂを考える。従来のデータ保管システムでは、利用者Ａが予め付与した電子署名を保管データと共に保管しておき利用者Ｂが参照したときにはその保管データと電子署名を利用者Ｂが検証する必要がある。このとき利用者Ｂは、異なる複数の利用者が保管したデータを参照する時、保管した人数分の公開鍵を取得しなければならない。そのため保管した利用者が多いほど取得しなければならない公開鍵の数が多くなるという問題がある。

【０００８】また、長期にわたり保管システムに保管してある場合には電子署名を検証するために必要な公開鍵の有効期限が切れていたり、利用者から無効化されていたりして検証結果が信用できなくなるという問題があった。以上のように、電子署名を用いたデータ保管を行うためにはデータを保管した利用者とは無関係なそして有効期限の影響を受けないデータの改竄検知方法を要する。

【０００９】この発明は、上記に鑑みてなされたもので、その目的とするところは、参照する利用者に多数の公開鍵を必要とさせず、公開鍵の有効期限切れや無効化による検証結果の信頼性の低下を防ぐデータの保管方法を提供することにある。

【００１０】

【課題を解決するための手段】上記目的を達成するため、この発明のデータ保管システムは鍵対の格納手段として電子署名作成鍵と検証鍵の両方を生成する手段と、電子署名作成手段と電子署名検証手段を有し、生成した鍵対（電子署名作成鍵と電子署名検証鍵）を内部に保持する。そして署名作成鍵で入力データの電子署名を生成出力する。また内部に保持したままの電子署名検証鍵は入力されたデータとそれに対応する電子署名を検証し検証結果を装置外部に出力する。

【００１１】また、この発明のデータ保管システムは、従来のデータ保管システムに加えて、データ保管サーバに通信用の電子署名作成鍵と保管用の電子署名作成鍵を別に有し、少なくとも保管用の電子署名鍵対は外部に公開しない鍵対の格納手段を有する。さらに、この発明のデータ保管方法はこの発明のデータ保管システムにおいて、保管データに対して保管利用者端末が付与した電子署名に加えて、保管サーバの保管用電子署名（これは保管データと利用者端末が作成付与した電子署名を合わせたものに対して作成される）を付与して保管し、保管データ参照時には保管用の電子署名を上記の鍵対格納手段

内で検証し、保管データに改竄がないことを確認後、保管用の電子署名のかわりに保管サーバで特定された通信用電子署名を上記の鍵対格納手段内で作成して付与し参照利用者端末に送信する。

【００１２】またさらに、この発明のデータ保管方法では参照利用者端末はデータ保管システムから受信したメッセージをデータ保管システムで定められた通信用検証鍵（公開鍵）を認証システムから取得してデータ保管システムの通信用電子署名を検証する。

（作用）以上のようにこの発明のデータ保管方法では利用者端末がデータを保管する時に自分の電子署名を付与してデータ保管システムに送信する。

【００１３】データ保管サーバは、受け取ったデータに改竄がないことを保管利用者の電子署名検証鍵により検証し、予め外部に出力されないように作成された電子署名作成鍵により作成された電子署名を付与して蓄積装置に保管する。利用者端末が保管データを参照する時に保管サーバは、予め外部に出力されないように鍵対格納手段内に作成された電子署名検証鍵によりその保管用の電子署名を検証し、保管データに改竄がないことを確認後、保管サーバで定められた通信用電子署名を保管データと保管利用者の電子署名の全体に対し付与して送信する。

【００１４】参照した利用者端末は、データ保管システムからの通信途中の改竄を検出するためにデータ保管サーバの通信用電子署名のみを検証することで通信途中の改竄の有無を確認する。

【００１５】

【発明の実施の形態】以下、図面を用いてこの発明の実施例を説明する。図１はこの発明の実施例を示す。データを保管しようとする利用者の端末３１は電子署名を作成するための関数演算を行う署名作成手段３２、電子署名を作成するための秘密鍵３３、データ保管サーバとの通信手段３４を備えている。データ保管システム３８が受信するデータ３５は保管しようとするデータの実態である保管データ３６と、通信時の改竄を検知するために保管利用者端末３１がデータ３６に対して作成した電子署名３７からなる。データ保管システム３８は、データ保管サーバ３９、電子署名装置４７、データ蓄積装置５４を備え、データ保管サーバ３９はデータ保管サーバ３９が外部と通信するための通信手段４０、公開鍵取得手段４１、保管利用者の公開鍵４２、電子署名検証手段４３、電子署名付与手段４４、この署名付与手段４４が電子署名を作成するときに利用される電子署名装置４７へのアクセス手段４５、データ蓄積装置アクセス手段４６を備えている。保管用鍵対の格納手段としての電子署名装置４７は、この電子署名装置４７内に予め格納された電子署名検証手段４８、電子署名装置４７の中で保持する電子署名作成鍵を用いた電子署名作成手段４９、鍵対（電子署名作成鍵と電子署名検証鍵）の生成手段５０を備え、データ保管サーバの通信用電子署名の作成鍵５１、データ保管サーバの保管用電子署名の作成鍵５２、データ保管サーバの保管用電子署名の検証鍵５３を有する。データ蓄積装置５４はデータ蓄積装置５４に蓄積されたデータ群（少なくとも保管データと保管利用者電子署名と保管サーバ電子署名からなる）５５を有し、データ群５５は保管データ３６に対応する保管データ５６、データ５６の保管要求者の電子署名５７、保管サーバ３９が電子署名装置４７を用いて作成した保管用電子署名５８よりなる。データ保管システム３８が送信するデータ５９は利用者端末が保管依頼したデータ６０、保管利用者がデータ６０に付与した電子署名６１、通信時の改竄を検知するためにデータ保管サーバ３９がデータ６０と６１を含んだ送信データ全体に対して作成した電子署名６２よりなる。参照利用者の端末６３は電子署名検証手段６４、公開鍵取得手段６５、データ保管サーバが付与した通信用電子署名６２を検証するための電子署名検証鍵６６、通信手段６７を備える。保管利用者および参照利用者およびデータ保管サーバの公開鍵証明証は認証システム６８に保管されている。

【００１６】次に図２を参照してデータ保管時の処理手順を説明する。今、利用者がデータを保管する場合を考える。その利用者の保管利用者端末３１は、保管データ３６と電子署名作成鍵３３を用いて電子署名作成手段３２により電子署名３７を作成する（ＳＴＥＰ２１）。そして少なくとも保管データ３６と電子署名３７を組み合わせてデータ保管システム３８で解釈できる形式のデータ３５として通信手段３４を用いてデータ保管システム３８に送信する。データ保管サーバ３９は通信手段４０を通してデータ３５を受信し（ＳＴＥＰ２３）、通信中のデータの完全性を確認するために、公開鍵取得手段４１により取得した保管利用者端末３１の公開鍵４２と受信したデータ３６および３７を入力として電子署名検証手段４３により検証する（ＳＴＥＰ２４）。この検証は問題がないことを確認した後、少なくとも保管データ３６と保管利用者の電子署名３７を入力として電子署名付与手段４４により保管用電子署名を作成指示し、電子署名付与手段４４は電子署名装置アクセス手段４５により電子署名装置４７に保管用の電子署名を作成指示する（ＳＴＥＰ２５）。

【００１７】電子署名装置４７は、入力された指示に従い保管用電子署名作成鍵５２を選択する（ＳＴＥＰ２６）。入力されたデータに対して電子署名作成手段４９は、鍵対生成手段５０により予め作成された保管用電子署名作成鍵５２を用いて保管用電子署名を作成する（ＳＴＥＰ２７）。作成した電子署名を呼出元の電子署名装置アクセス手段４５に返却する（ＳＴＥＰ２８）。

【００１８】データ保管サーバ３９は、電子署名装置４７から返却された保管用電子署名５８を保管データ５６と保管利用者署名５７と対応付けてデータ群５５として

データ蓄積装置アクセス手段４６によりデータ蓄積装置５４に格納する（ＳＴＥＰ２９）。次に図３乃至図６を参照してデータ参照時の処理手順を説明する。

【００１９】今、利用者がすでに保管されているデータ５６を参照する場合を考える。図３に示すようにデータ保管サーバ３９は、参照利用者端末６３から参照要求を受け取る（ＳＴＥＰ３０）。それから蓄積装置アクセス手段４６を用い参照要求に指定されたデータ５６を含むデータ群５５を読み込む（ＳＴＥＰ３１）。読み込んだデータ群５５に改竄がないことを検証するため電子署名装置アクセス手段４５により電子署名装置４７に検証依頼する（ＳＴＥＰ３２）。

【００２０】電子署名装置４７は、図４に示すように入力指示に従って鍵対生成手段５０により予め作成された保管用電子署名検証鍵５３を選択する（ＳＴＥＰ３３）。入力されたデータ５５と保管用電子署名の検証鍵５３と電子署名検証手段４８を用いて検証する（ＳＴＥＰ３４）。その検証結果（ＯＫまたはＮＧ）を電子署名装置アクセス手段４５に返却する（ＳＴＥＰ３５）。

【００２１】データ保管サーバ３９は、電子署名装置４７からの返却値がＯＫであることを確認した後、図３に示すように保管データ５６と保管利用者の電子署名５７を電子署名付与手段４４により電子署名装置４７に対し通信用電子署名の作成要求をする（ＳＴＥＰ３６）。電子署名装置４７は、入力指示に従って鍵対生成手段５０により予め作成された通信用電子署名作成鍵５１を選択する（図４ＳＴＥＰ３７）。入力されたデータに対して通信用電子署名作成鍵５１を用いて電子署名作成手段４９で通信用電子署名６２を作成しそれを電子署名装置アクセス手段４５に返却する（ＳＴＥＰ３８）。

【００２２】データ保管サーバ３９は、図３に示すように保管用電子署名５８の代わりにＳＴＥＰ３８で返却された保管サーバの通信用電子署名６２を付与し、データ群５９として通信手段４０によりデータ参照利用者端末６３に送信する（ＳＴＥＰ３９）。データ参照利用者端末６３は、図５に示すように通信手段６７によりデータ群５９を受信し（ＳＴＥＰ４０）、その後データ保管サーバの正しい電子署名検証鍵６６を公開鍵取得手段６５により認証システム６８から取得し（ＳＴＥＰ４１）、受信したデータ群５９に改竄がないことを電子署名検証手段６４を用いて通信用電子署名６２を検証する（ＳＴＥＰ４２）。このとき、受信したデータ５９は図６に示すような関係を保持しており、通信用電子署名６２は保管データ６０と保管利用者の電子署名６１の正しい関係を保持したまま作成されているためＳＴＥＰ４２の検証結果がＯＫであることは保管利用者の電子署名６１の検証結果がＯＫであることも意味しており、取得したデータ６０が保管利用者端末が保管したデータと同一であることも同時に検証したことを意味する。

【００２３】この実施例では、保管用の電子署名作成手段および検証手段として公開鍵暗号方式の鍵対を用いて説明したが、保管用電子署名の作成および検証手段としては共通鍵暗号方式による鍵を利用しても同様の効果を得ることができる。またデータ保管システムでの各処理はコンピュータがプログラムを解読実行することにより行わせることもできる。

【００２４】

【発明の効果】以上説明したように、この発明によれば保管した利用者の数が多数になっても参照する利用者が必要とする公開鍵はデータ保管サーバの公開鍵のみであり、その通信データの改竄検証を行うだけで同時に参照したデータとそれが保管されたときのデータとの同一性を確認できる。同時に、必要とする公開鍵数が少なくなることから認証システムへのアクセス回数を削減する効果がある。

【００２５】また、データ保管サーバが電子署名装置内に電子署名の作成鍵と検証鍵の両方を格納し、外部には公開しないことで一般の電子署名用鍵対を用いた改竄検知手段よりも有効期限を長くすることができ、かつ認証システムにより公開されないため公開鍵の有効期限切れや利用者による鍵の無効化に伴う検証結果の信頼性の低下を防ぐデータの保管方法を提供することができる。

【図面の簡単な説明】

【図１】この発明のデータ保管システムの機能構成の実施例を示す図。

【図２】この発明の利用者端末と保管サーバでのデータ保管時の処理フローを示す図。

【図３】この発明の利用者端末と保管サーバでのデータ参照時の保管サーバ側の処理フローを示す図。

【図４】データ参照時の電子署名装置側の処理フローを示す図。

【図５】データ参照時の参照利用者端末側の処理フローを示す図。

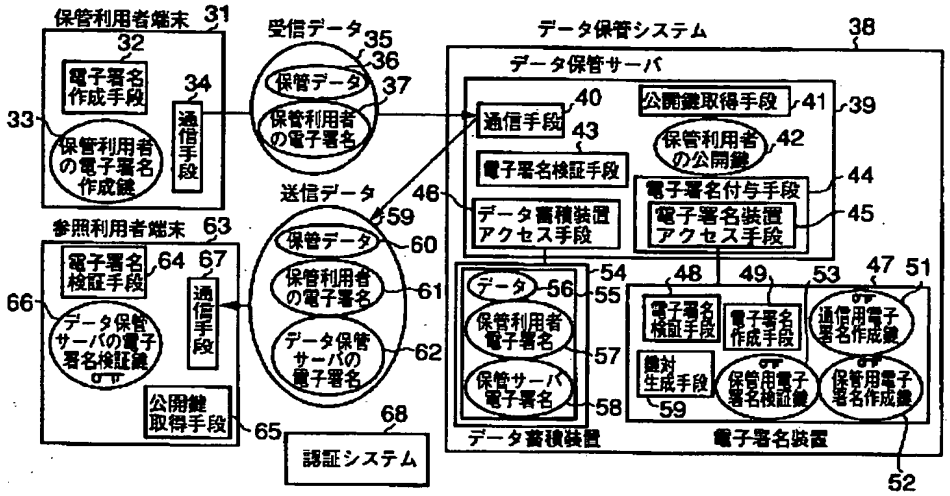
【図６】この発明の実施例でのデータと電子署名の対応を示す図。

【図７】データ保管のための従来装置の機能構成を示す図。

【図８】従来の利用者端末と保管サーバでのデータ保管時の処理フローを示す図。

【図９】従来の利用者端末と保管サーバでのデータ参照時の処理フローを示す図。

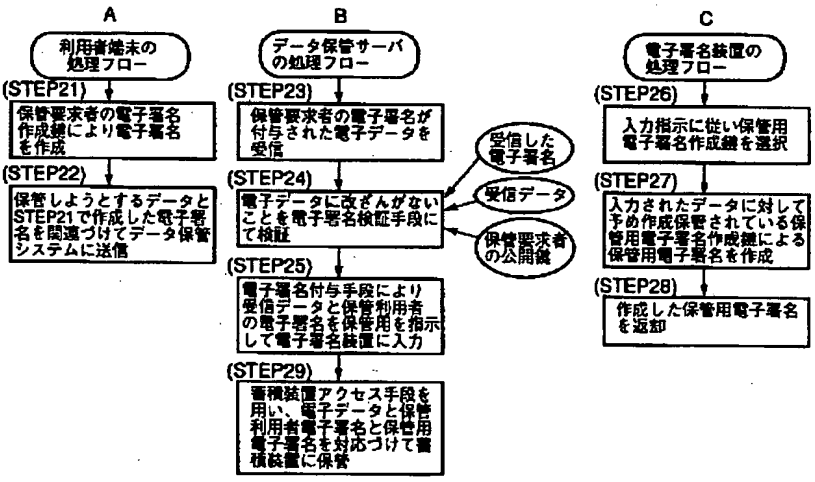
【図１】



本発明のデータ保管システムの装置構成の実施例

図　1

【図２】



本発明の利用者端末と保管サーバでのデータ保管時の処理フロー

図　2

【図３】

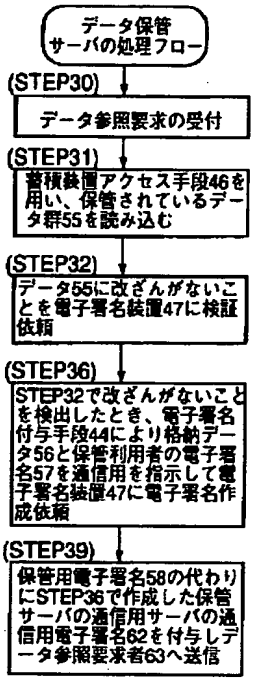


図　3

【図５】

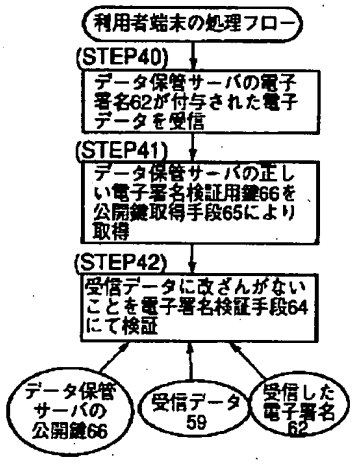


図　5

BEST AVAILABLE COPY

【図４】

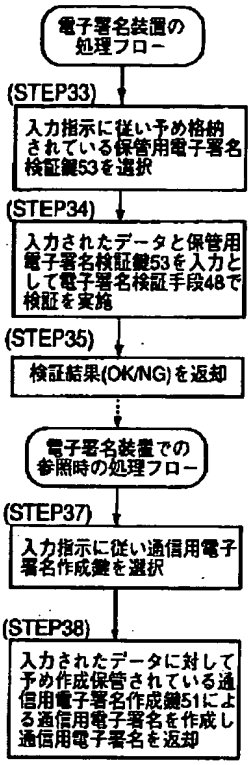
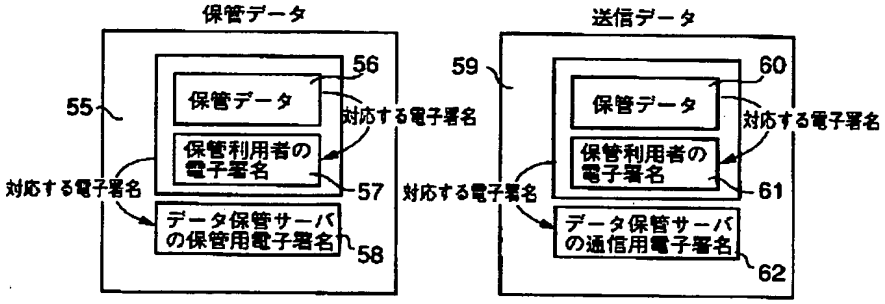


図　4

【図６】



データと電子署名の対応

図　6

【図７】

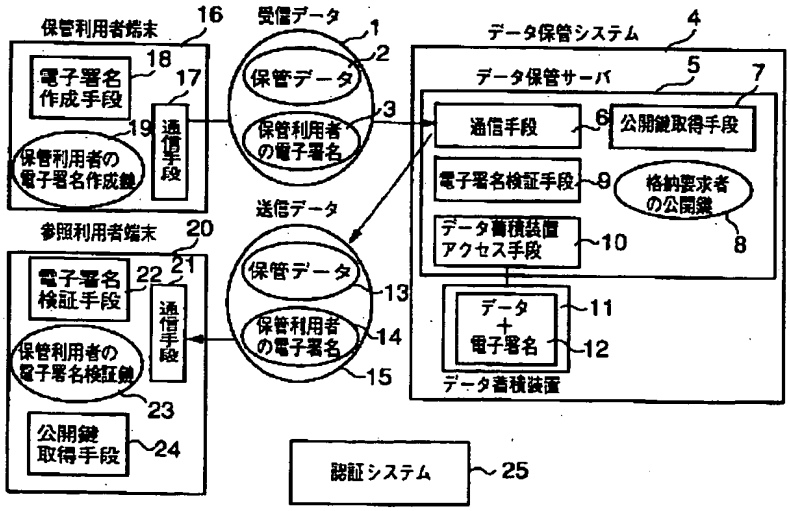
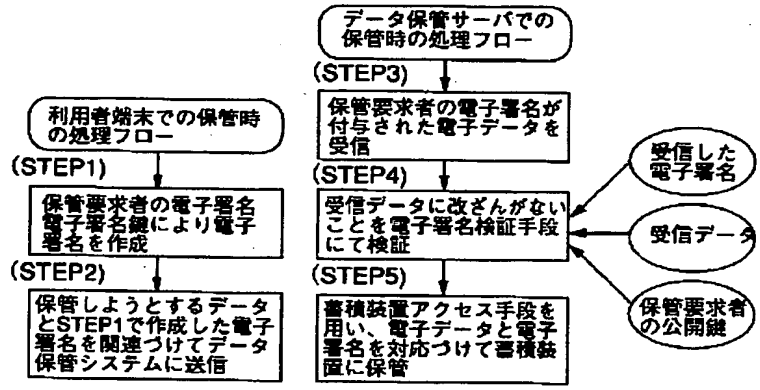


図　7

BEST AVAILABLE COPY

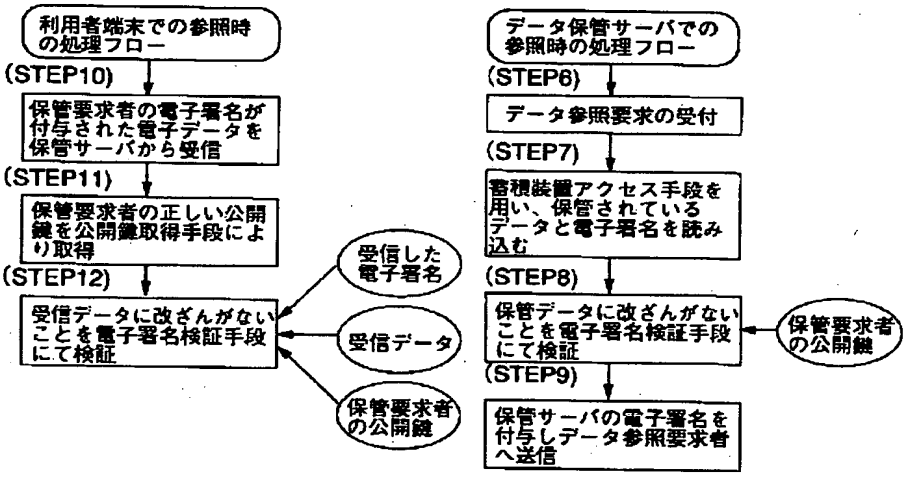
【図８】



従来の利用者端末と保管サーバでのデータ保管時の処理フロー

図　8

【図９】



従来の利用者端末と保管サーバでのデータ参照時の処理フロー

図　9

BEST AVAILABLE COPY